修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報理工学研究科　情報学専攻　博士前期課程		
氏　　名	羽田野　凌太	学籍番号	1930097
論 文 題 目	レーザー攻撃検知回路 BBICS の安全性評価		

要　旨

暗号ハードウェアにレーザーを照射して故障を誘発させる Laser Fault Injection(LFI)攻撃が脅威とされている. その対策として, Bulk Built-In Current Sensor(BBICS)というレーザー攻撃検知回路を統合した AES 暗号チップが提案された. BBICS では, レーザーを照射した際に暗号回路内に発生する電流を検知し, アラーム信号を出力する.　本研究では BBICS を統合した AES 暗号チップに対して, サイドチャネル攻撃耐性の評価を行う. 実験では, BBICS から出力されたアラーム信号が中間値の HW と依存性をもつことを示した. また, アラーム信号を用いた相関解析と故障感度解析を行い, 秘密鍵を復元した. 実験結果から, アラーム信号は暗号化計算の情報を漏洩していることを示した. さらに, BBICS の回路からアラーム信号が情報を漏洩する原因を考察し, 情報漏洩を防ぐ対策について考察を行った. 最後に, BBICS を含めた LFI 攻撃検知回路技術の特徴をまとめ, それぞれの特性について評価を行った.

令和二年度修士論文

レーザー攻撃検知回路BBICSの安全性評価

情報学専攻　セキュリティ情報学プログラム

1930097　羽田野 凌太

主任指導教員　崎山 一男 教授

指導教員　李 陽 准教授

2021年1月25日

目次

1 はじめに **1**

1.1 背景 1

1.2 本論文の構成 2

2 先行研究 **4**

2.1 フォールト解析 4

2.1.1 差分故障解析 4

2.1.2 Ineffective Fault Analysis 5

2.2 故障注入方法 5

2.2.1 クロックグリッチ 5

2.2.2 レーザーフォールトインジェクション攻撃 5

2.3 リーケージモデル 6

2.3.1 ハミングディスタンスモデル 6

2.3.2 ハミングウェイトモデル 6

2.4 相関電力解析 7

2.5 故障感度解析 7

3 BBICS を統合した AES 暗号チップ **8**

3.1 BBICS 8

3.2 LFI 攻撃に対する耐性 9

4 BBICS を統合した AES 暗号チップの脆弱性評価 11

4.1 IFA 耐性評価 11

4.2 アラーム信号による情報漏洩評価実験 12

4.2.1 実験のセットアップ 12

4.2.2 実験で用いられたアラーム信号 13

4.2.3 アラーム信号におけるリーケージモデル 14

4.3 アラーム信号を用いた相関解析に対する耐性評価 15

4.4 FSA に対する耐性評価 17

5 議論 19

5.1 アラーム信号と中間値の HW との依存性に関する考察 19

5.2 対策 23

6 LFI 攻撃検知技術の特徴 24

7 結論 28

第1章

はじめに

1.1 背景

近年，IoT 化が進み，様々なデバイスがインターネットと接続を行い，情報通信が行われている．その際のセキュリティ要件を満たすために，暗号技術は様々な電子機器で用いられており，情報漏洩を目的とした攻撃を防ぐことに利用されている．暗号技術に用いられる暗号は，計算量的安全性を満たす必要がある．しかし，暗号を電子機器に搭載する際には，計算量的安全性だけでは十分ではなく，物理攻撃に対する耐性が必要とされる．主な物理攻撃の例として，暗号デバイスの電力消費などから情報を取得するサイドチャネル攻撃が挙げられる [2]．また，暗号デバイスに対して物理的に攻撃を行い，一時的な故障を発生させることで秘密鍵を取得する差分故障解析 (Differential fault analysis:DFA) も有力な攻撃方法として考えられる [3]．差分故障解析では，暗号計算の途中に故障を発生した時に得られる誤り暗号文と正常時に出力される暗号文を用いて，秘密鍵を導出する．先行研究では，差分故障解析を行った時に漏洩する情報量について研究がされている [4, 5]．これに対し，故障感度解析 (FSA) は，誤り暗号文を必要としない攻撃方法である [6]．故障感度解析 (Fault Sensitivity Analysis:FSA) では，故障が発生し始める故障誘発要因の強さと中間値の依存性を利用して，

*本論文は，同著者他らによる電子情報通信学会論文誌 (A) に投稿した“ LFI 検知回路に対するサイドチャネル攻撃耐性評価 ”[1] に基づきます．

秘密鍵を導出する．差分故障解析や故障感度解析は，故障を誘発させることで秘密鍵の情報を取得することができるため，暗号デバイスに故障を誘発させる攻撃シナリオは特に脅威とされている．

具体的に暗号デバイスに故障を誘発させる方法としては，クロックグリッチを挿入する方法，レーザーを照射する方法が挙げられる [7, 9]．特にレーザーを照射する方法では，攻撃者は故障を発生させるタイミングとビットの位置を正確に制御することができるため，最も強い故障誘発方法の一つとして考えられる．この攻撃をレーザーフォールトインジェクション (LFI) 攻撃と呼ぶ．

暗号デバイスの物理攻撃に対する耐性を高めるため，先行研究ではサイドチャネル攻撃に対する対策方法について多くの研究がされている [10, 11, 12, 13, 14, 15, 16, 17, 18]．主な対策方法としては，暗号アルゴリズムに対策を施すものと暗号デバイスに対策を施すものがある．暗号アルゴリズムに対策を施すものとしては，ハイディングやマスキングなどが挙げられる [10, 11]．暗号デバイスに対策を施すものとしては，攻撃を検知するものがある．2018 年に，現在最も多く使用されている共通鍵暗号の Advanced Encryption Standard (AES)[19] に対し，LFI 攻撃を検知する対策を施したチップが提案された [18]．このチップは，AES 暗号回路と Bulk Built-In Current Sensor (BBICS) というセンサーを統合することによって，LFI 攻撃によって発生する大電流を検知する．検知後にレーザー照射を検知したことを示すアラーム信号を発し，チップ内のデータを瞬時に消去することで情報漏洩を防ぐ．本研究では，[18] で提案された BBICS を統合した AES 暗号チップにサイドチャネル攻撃を行い，BBICS の安全性評価を行う．

1.2 本論文の構成

本論文は，次の章から構成される．第 2 章では，サイドチャネル攻撃に関する先行研究について述べる．第 3 章では，[18] で提案された LFI 攻撃を検知する対策を施したチップの詳細

やBBICSについてまとめる．第4章では，BBICSを統合したAES暗号チップに対する脆弱性評価を行う．第5章では，BBICSを統合したAES暗号チップの脆弱性の原因や対策について議論を行う．第6章では，LFI攻撃検知技術の特徴についてまとめる．第7章では，本研究をまとめ，結論を述べる．

第2章

先行研究

2.1 フォールト解析

本節では，フォールト解析についてまとめる．フォールト解析はサイドチャネル攻撃の一つである．攻撃者は暗号ハードウェアに対し，計算誤り（フォールト）を誘発させ，その挙動を観測することで暗号鍵を導出する．フォールト解析には，差分故障解析と Ineffective Fault Analysis(IFA) がある．

2.1.1 差分故障解析

差分故障解析では，正常な計算結果を出力した暗号文とフォールトを注入した誤り暗号文を 1 ペアとして攻撃を行う．ここではフォールトモデルを指定できる攻撃者を想定する．よって，誤り暗号文は，攻撃者が指定したフォールトモデルに基づく暗号文である．攻撃者は，鍵を予測し，正常な暗号文と誤り暗号文に対し，逆演算を行う．逆演算後の値がフォールトモデルに従うか否かで，予測した鍵が真の鍵であるかを判断する．もし仮に，一回の攻撃後に 2 つ以上の鍵が候補として考えられる場合には，新たに誤り暗号文を取得し，同様の解析を行う．鍵空間から鍵を一つに絞ることができれば，その鍵を真の鍵として推定することができる．現在最も汎用的に用いられている暗号の一つである AES 暗号 [19] に対しての差分故障解析では，正しい暗号と誤り暗号文のペア 2 組で 128 ビットの鍵を導出することができる [21].

2.1.2 Ineffective Fault Analysis

IFA では，差分故障解析と同様にレーザーを用いてフォールトを注入するような攻撃者を想定する．フォールトモデルは暗号文の計算途中の値を 0 に固定する (Stack at 0) フォールトモデルが考えられる．Stack at 0 フォールトモデルの場合，故障注入前の暗号文の中間値が 1 であれば，故障を発生させた後，0 に遷移する．中間値が 0 であれば，故障を発生させた後の暗号文に変化がない．攻撃者は，フォールトを注入したにも関わらず，計算結果が変わらなかったときの情報を用いて，秘密鍵の解析を行う．このように，フォールトが計算結果に影響しないことを無影響故障といい，それを用いたフォールト解析をセーフエラー型という．先行研究では，ビットフリップ検知機能の悪用により IFA を実現する方法が報告されている [30].

2.2 故障注入方法

2.2.1 クロックグリッチ

クロックグリッチは，攻撃者がクロック信号に対してグリッチと呼ばれるパルス状のノイズを仕掛けることで，故障を起こす攻撃である [7, 8]．暗号回路を設計する際，クロック信号の周期は全ての回路の最大遅延時間よりも長い時間に設定をする．クロック信号の周期が最大遅延時間よりも短くなってしまうとセットアップタイミング違反が起こってしまい，データが破損してしまう．クロックグリッチは，グリッチと呼ばれる短い立ち上がりの信号をクロック信号に挿入することで，セットアップタイミング違反を誘発させる．

2.2.2 レーザーフォールトインジェクション攻撃

LFI 攻撃は，故障を発生させる時間とビットの位置を制御できる点から特に脅威として考えられる．[22] では，レーザー照射によって起こる現象と発生する故障のモデルが分析されて

いる．LFI 攻撃では，攻撃者はシリコン基板にレーザーを照射することで，正孔と電子を再結合させる．再結合によって PN 接合間に再結合電流が流れる．再結合電流が大きくなると，電源とグランド間で短絡が発生し，中間値を変更することができる．

レーザーを照射する箇所に適切な強度のレーザーを照射することができれば，攻撃者は任意の中間値ビットの値を変更することができる．そのような攻撃者を想定した場合，得られる情報量は多くなるため，少ない攻撃回数で秘密鍵を復元することができる．

2.3 リーケージモデル

サイドチャネル攻撃は，物理的な情報漏洩（リーケージ）を用いた攻撃法である．代表的なリーケージモデルとして考えられるのが，ハミングディスタンスモデルとハミングウェイトモデルの二つである．二つのリーケージモデルは多くの研究で，消費電力と相関があることが示されている．

2.3.1 ハミングディスタンスモデル

ハミングディスタンスモデルは入力の遷移に応じた消費電力の変化をリーケージとする．CMOS の物理特性から，0 と 1 の切り替え時に貫通電流が発生する．ある処理の前後に，0 と 1 の切り替えが発生する場合としない場合では，切り替え発生時の方が消費電力が多くなる．よって，消費電力を計測することでレジスタの値の変化がわかる．[23] では，ハミングディスタンスモデルを用いて，電力波形から鍵を推定している．

2.3.2 ハミングウェイトモデル

CMOS では，値が 1 であることを示すのに，コンデンサへの電子の電荷を必要とする．値の 0 を示すときには，電子の放出が行われる．この 1 ビットに注目したシングルビットモデルを全てのビットに拡張したものがハミングウェイトモデルである．全てのビット中にある値

1 の数が多いほど，多くの電子の電荷を必要とし，値 0 の数が多ければ，電子の放出量が多くなる．よって，消費電力と中間値の 1 の数が相関する．[24] では，ハミングウェイトモデルを用いて，電力解析攻撃に対する脆弱性を示した．

2.4 相関電力解析

サイドチャネル攻撃の一つとして電力解析攻撃がある．電力解析攻撃は，ハードウェアが暗号化計算をしているときに，その消費電力が暗号化計算の内容によって変化することに基づいて行われる攻撃である．その中でも，相関電力解析は，予測リーケージと測定した消費電力との相関係数を求めて，暗号鍵を求める攻撃である [23]．予測リーケージは，ハードウェアのリーケージモデルを予測し，予測鍵を用いて計算される．各暗号鍵に対応する中間値とリーケージモデルの相関係数を比較して，暗号化計算に用いられた暗号鍵を特定することができる．

2.5 故障感度解析

FSA は，論理回路の伝播遅延が入力値に依存することを利用した鍵復元攻撃である [6]．攻撃者はクロックグリッチを挿入し，セットアップタイミング違反を発生させ，一時的な故障を引き起こす．中間値によって暗号回路内の伝播遅延は変化するため，故障の発生のしやすさ（故障感度）は中間値に依存する．この依存性を利用して鍵を復元する．先行研究では，LFI 攻撃を用いた FSA が提案され，実証実験により鍵復元可能なことが示されている [25]．FSA では，故障発生後に出力される誤り暗号文を必要としない．必要な情報は故障が発生したか否かの情報のみであり，DFA と比較して，攻撃者に求める能力が低いという特徴がある．

第3章

BBICSを統合したAES暗号チップ

本章では，BBICS を統合した AES 暗号チップ [18] に対して述べる．このチップは LFI 攻撃検知機能を備えた AES 回路である．LFI 攻撃検知機能は BBICS というセンサーを用いて行なっており，BBICS の詳細を第 3.1 節で言及し，LFI 攻撃に対する耐性について，第 3.2 節で言及する．

3.1 BBICS

本節では，Bulk Built-In Current Sensor(BBICS) について述べる．第 2.2.2 節で言及したように LFI 攻撃では，PN 接合間に再結合電流を流し，短絡を起こす必要がある．BBICS は，この短絡によって発生する大電流を検知する [26]．BBICS の回路を図 3.1 に示す．INNWELL，INPWELL はそれぞれ PMOS と NMOS に接続されており，両方の MOS を監視することができる．OUT が ON 状態になると，攻撃が検知されたことを示す．

NMOS に LFI 攻撃されたときの BBICS について説明を行う．NMOS にレーザーが照射され，NMOS が ON 状態になり，短絡が発生する．この短絡によって大電流が流れると INPWELLL の電圧が上昇する．そして，トランジスタが OFF 状態から ON 状態に切り替わる．この切り替わりによって，OUT が ON 状態になり，攻撃を検知する．

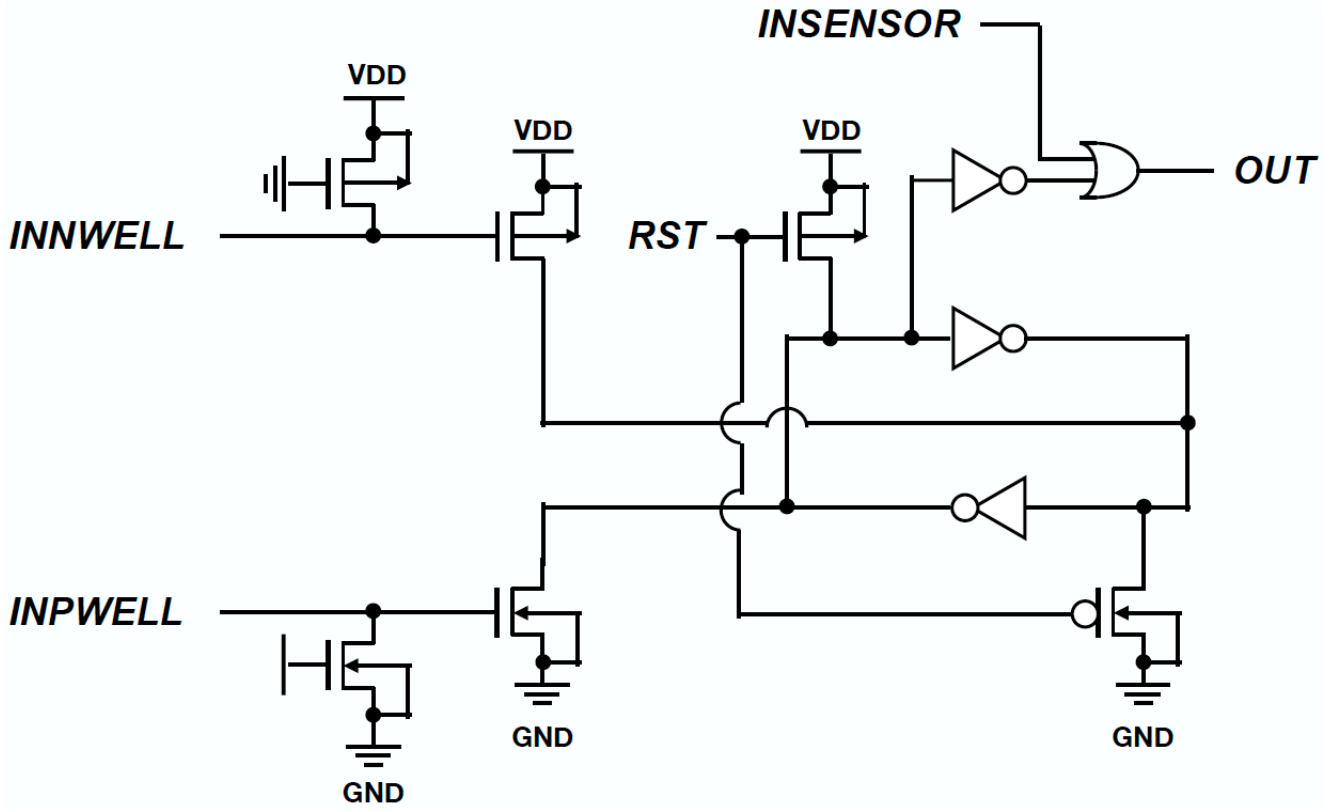

図 3.1：BBICS の回路

3.2 LFI 攻撃に対する耐性

[18] で提案されたチップでは，第 3.1 節で示した BBICS を統合している．BBICS というセンサーを AES 暗号に直接統合することによって，AES 暗号チップへの攻撃を検知することができる．統合を行わずに，AES 暗号チップとレーザー照射を検知するセンサーを別々のモジュールとして設計すると，レーザーの照射精度によって，AES 暗号チップだけを狙って攻撃することができてしまうため，情報が漏洩してしまう．

LFI 攻撃がされたとき BBICS では，BBICS 内の OUT が ON 状態になり，攻撃を検知する．提案されたチップでは，BBICS 内の OUT が ON 状態になると，アラーム信号を出力する．その後，即時に AES コアへの電源供給をシャントすることで，内部のデータを消去する．レーザー照射による再結合電流を検知した時点で内部のデータを消去するため，誤り暗号文の出力を防ぐことができる．よって，差分故障解析を防ぐことができる．また，BBICS が検知できる電流の下限は，故障を発生させるために必要な電流の強さに対し，十分に小さ

い．よって，故障が発生したかどうかに関わらず，レーザーが照射されればアラーム信号を出力する．そのため，BBICS を統合した AES 暗号チップは，故障が発生しない場合でも攻撃を検知することができるため，IFA に対しても有効な対策といえる．

第4章

BBICSを統合したAES暗号チップの脆弱性評価

本章では，BBICS を統合した AES 暗号チップ [18] に対して脆弱性評価を行う．第 4.1 節では，先行研究 [27]．で行われた IFA 攻撃への耐性評価について言及する．第 4.2 節では，BBICS を統合した AES 暗号チップから出力されたアラーム信号を用いて，情報漏洩の評価を行う．第 4.3 節では相関解析に対する耐性評価，第 4.4 節では FSA に対する耐性評価を行う．

4.1 IFA 耐性評価

先行研究では，LFI 攻撃対策が施された AES 暗号チップに対する Ineffective Fault Analysis (IFA) が提案されている [27]．IFA は，暗号デバイスに故障を起こすだけの物理的操作をチップに与えたにも関わらず，故障が発生しないという情報を用いた鍵復元攻撃である [28]．内部データを強制的に 0 にするようなフォールトモデルを考えた場合，攻撃前の内部データが 1 のときは攻撃後に 0 に変化する．しかし，内部データが 0 のときは攻撃前後の内部データの変化がない．LFI 攻撃の場合，内部データが変化した場合にのみ回路内に短絡が発生する．BBICS は短絡による大電流を検知するため，内部データが変化する場合のみ攻撃を検知することができる．[27] では，この BBICS の LFI 攻撃検知機能と内部データの依存性により，IFA が行えることを理論的に示している．IFA を実行するには，任意の中間値をビット

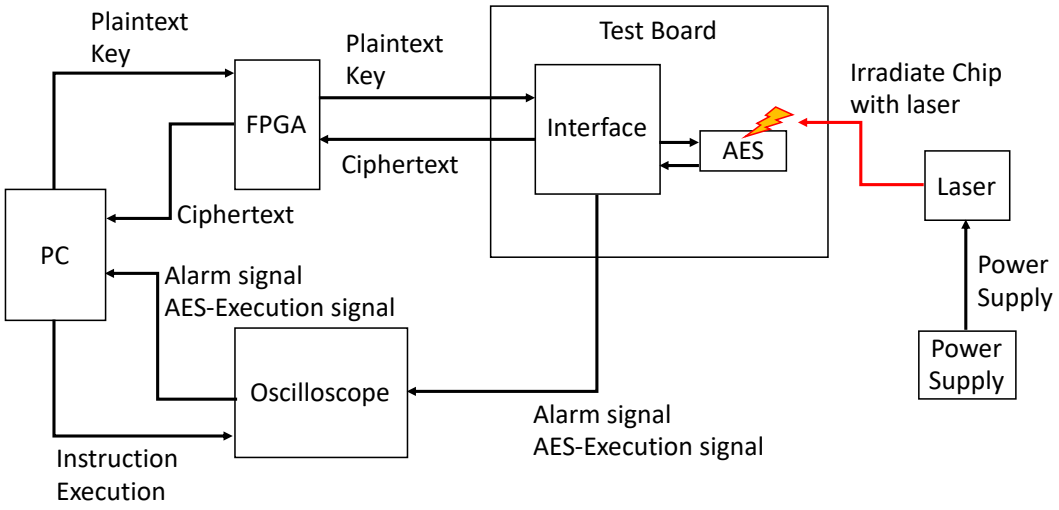

図 4.1：実験環境

フリップできるほどの正確なレーザー制御能力を必要とする．

4.2 アラーム信号による情報漏洩評価実験

4.2.1 実験のセットアップ

実験の実験系を図 4.1 に示し，AES 暗号チップにレーザーを照射している様子を図 4.2 に示す．用いられた実験器具を表 4.1 に示す．実験では，対象の BBICS を統合した AES 暗号チップに実際にレーザーを照射し，出力されるアラーム信号について分析が行う．レーザーは安定化電源に接続されており，出力電圧を変更できるため，レーザーの強度を変更することができる．PC で設定した鍵や平文を AES 暗号チップで暗号化し，暗号文が PC に出力される．実験では，IO ピンから AES-Execution 信号とアラーム信号の二つの信号をオシロスコープを用いて取得している．AES-Execution 信号は，AES の暗号化計算が行われているときに HIGH になる信号である．アラーム信号は，BBICS が異常電流を検知した際に HIGH になる信号である．AES-Execution 信号をトリガーとして使用し，アラーム信号の取得を行う．

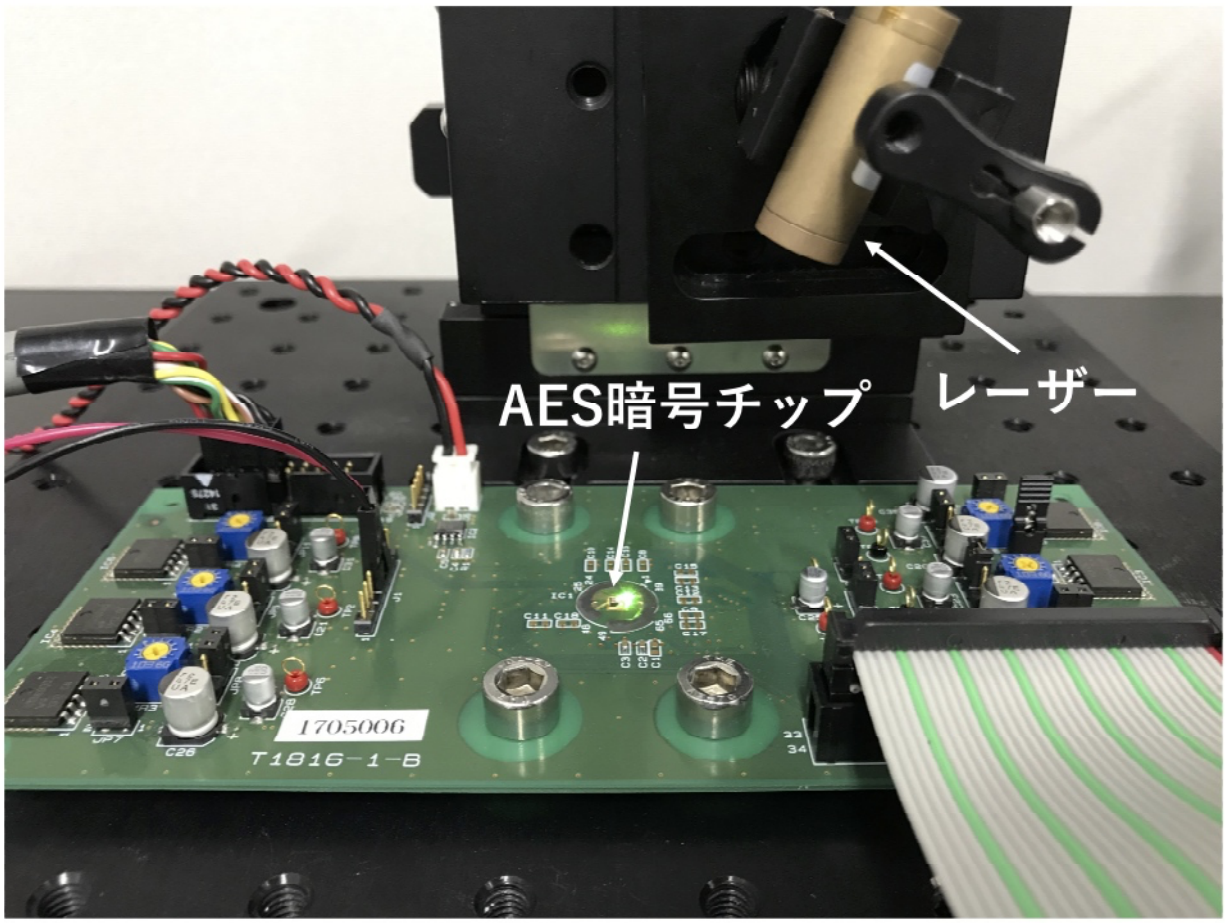

図 4.2：実験のセットアップの写真

4.2.2　実験で用いられたアラーム信号

第 4.2.1 節のように実験環境を設定し，チップにレーザーを照射して得られるアラーム信号は，安定的な HIGH か LOW の信号である．アラーム信号が出力する安定的な HIGH と LOW の信号は，レーザーの強度に大きく依存していると考えられる．よって，そのようなアラーム信号から AES 暗号の計算情報の漏洩は考えにくい．そこで，不安定な波形が出力されるようにレーザーの照射位置とレーザーの強度の調整を行う．その結果，図 4.3 のような波形が得られた．図 4.3 の緑色の波形が AES-Excecution 信号を示す．黄色の波形がアラーム信号を示す．図 4.3 より，アラーム信号の出力が小刻みに上下していることが観察できる．これは，アラーム信号が LOW から HIGH になる閾値ほどの再結合電流がレーザー照射によって流れていることが原因だと考えられる．よって，この信号はレーザー強度による影響が最も小さ

表 4.1：実験器具

FPGA	Xilinx SPARTAN XC3S1400AN[29]
オシロスコープ	Agilent DSO7032A
レーザー	Lightvision Technologies JPM-1-3(A4)
供給電源	菊水 PMC18-2A

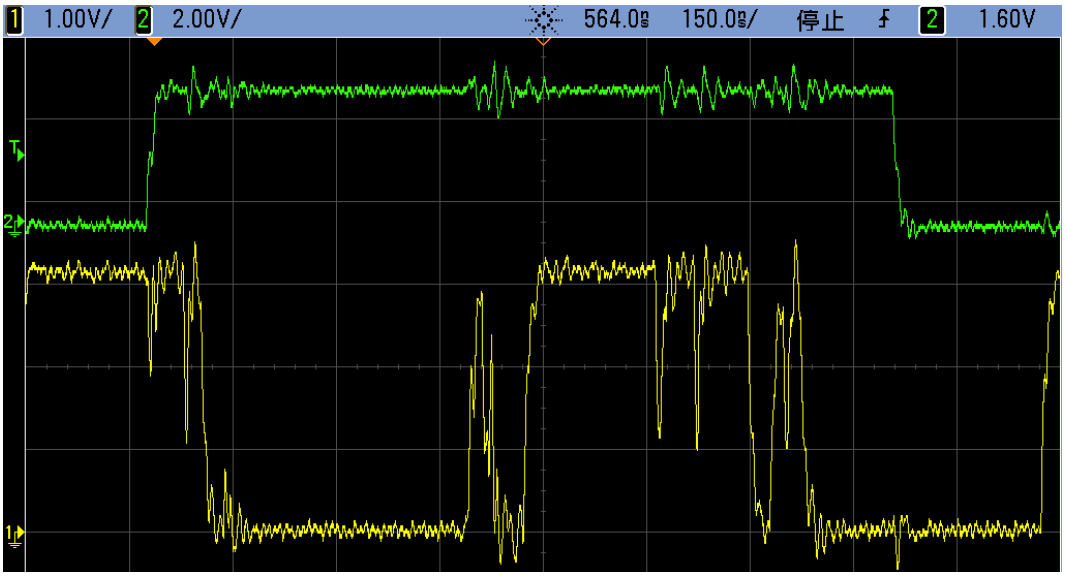

図 4.3：実験で用いた AES-Execution 信号 (上) とアラーム信号 (下)

く，計算情報を漏洩している可能性が最も高いと推測できる．

4.2.3 アラーム信号におけるリーケージモデル

第 4.2.2 節で情報漏洩が予想されたアラーム信号が，実際に情報を漏洩しているのかどうかを確かめるために実験が行う．実験では，第 2.3 節で述べたリーケージモデルとアラーム信号の相関関係について評価を行う．相関関係があった場合，アラーム信号が暗号化計算の情報を漏洩していると考えられる．相関関係は，AES 暗号の中間値を取得し，そのリーケージモデルとアラーム信号の電圧との相関係数を計算することによって評価する．相関係数は 128 ビットの中間値を用いて計算する．

実験では，アラーム信号の波形を 36.2 万波形用いて，1 ラウンド目と 10 ラウンド目の入力のハミングウェイト，10 ラウンド目の入出力のハミングディスタンスとの相関係数を計算

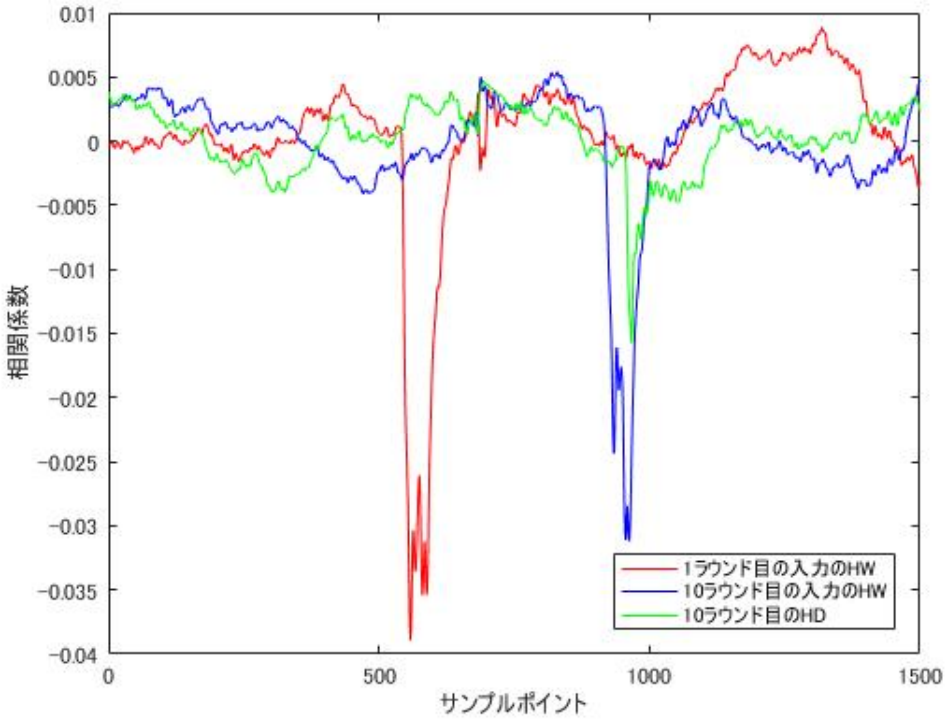

図 4.4 : アラーム信号の電圧と各リーケージモデルの相関関係

した．実験結果を図 4.4 に示す．この結果から，アラーム信号の電圧がラウンド入力のハミングウェイトに大きく依存していることがわかる．また，アラーム信号の電圧とラウンド入力のハミングウェイトは負の相関があると考えられる．リーケージモデルを比較すると，ハミングディスタンスよりもハミングウェイトの方が強い相関関係がみられる．よって，攻撃に用いるとすれば，ラウンド入力のハミングウェイトが妥当であると考えられる．また，サンプルポイントに注目すると，600 ポイント付近で AES 暗号の 1 ラウンド目と相関が見られ，900 ポイント付近で 10 ラウンド目と相関があることが確認できる．

4.3　アラーム信号を用いた相関解析に対する耐性評価

前節でアラーム信号の電圧波形はラウンド入力のハミングウェイトに依存していることを示した．しかし，前節では，128 ビットの中間値と電圧波形の相関を示している．128 ビットの鍵を予測して暗号鍵を求めるのは，総当たり攻撃と同等な計算量を必要とする．128 ビット

Algorithm 1 アラーム信号を用いた相関解析

Input: アラーム信号の電圧波形 V^j, 暗号文 C_b^J
Output: AES の最終ラウンドの鍵 K_b

for $K_b = 0$ to $2^8 - 1$ **do**
  for i = 1 to N **do**
    $I_b[i] \leftarrow S^{-1}(C_b^i \oplus K_b)$
    $L_b[i] \leftarrow HW(I_b[i])$
  end for
  $KeyList[K_b] \leftarrow \rho(V, L_b)$
end for
return $K_b \leftarrow max_{K_b} KeyList[K_b]$

の鍵を予測する方法は計算量の観点から現実的ではない．そこで本節では，8 ビットの鍵を予測して，相関解析を行い，鍵を復元できるか検証を行う．実験では，AES 暗号の暗号化計算時のアラーム信号と暗号文を得ることができる攻撃者を想定している．また，攻撃者はレーザーを照射し，図 4.3 のような不安定な波形を出力できるとする．アラーム信号を用いた相関解析のアルゴリズムを Algorithm1 に示す．攻撃者は暗号文を得て，10 ラウンド目の暗号鍵を予測し，暗号鍵と対応する 10 ラウンド目の入力値を計算する．その入力値とアラーム信号の電圧との相関係数を計算し，秘密鍵を導出する．Algorithm1 の入力の V は，チップ内に分散されている全ての BBICS からのアラーム信号を結線したときの電圧を示している．

実験では，前節と同様に 36.2 万波形のアラーム信号の波形を用いて，相関解析を行った．実験結果を図 4.5 に示す．鍵空間は 8 ビットであり，黒線が正解鍵の相関係数，灰色の線が偽鍵の相関係数を示す．結果より，サンプルポイントの 900 ポイント付近で正解鍵の相関係数が突出して低いことがわかる．このデータは AES-128 の暗号鍵全 16 バイト中の 1 バイトの結果を示したものであるが，他の 15 バイトでも同様に正解鍵の相関係数は突出して低いという結果が得られた．これらのことから，アラーム信号の波形を 36.2 万波形用いた鍵復元は十分に可能であると言える．

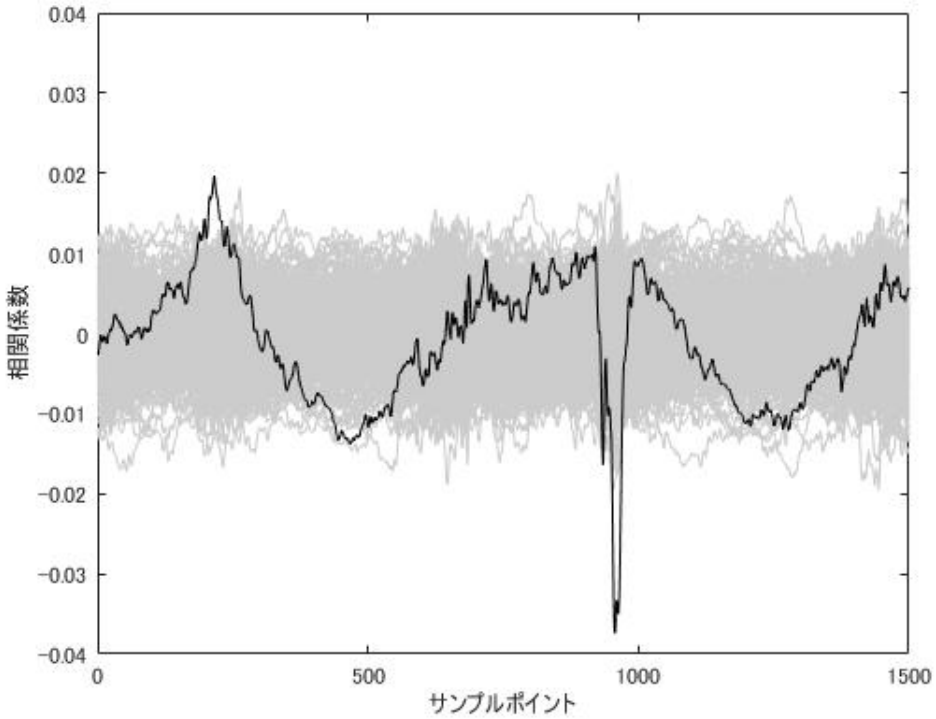

図 4.5：相関解析結果

4.4 FSA に対する耐性評価

本節では，BBICS を統合した AES 暗号チップに対する FSA の耐性について評価を行う．第 2.5 節で言及したように，FSA に用いる情報は故障が発生したか否かという情報である．本稿では，アラーム信号の出力を，故障が発生したか否かという情報と捉え，FSA を試みる．第 4.3 節の相関解析との違いは，相関解析ではアラーム信号の電圧の連続的データを用いるのに対し，FSA では，アラーム信号の ON と OFF という離散的データを用いる点である．よって，相関解析よりも攻撃者に求める能力が低いといえる．

実験では，第 4.3 節の相関解析に用いたアラーム信号の波形を使用する．アラーム信号の電圧に対し，閾値を設定して，閾値を境にして，アラーム信号の ON,OFF を定義する．アラーム信号の ON の電圧は 3.3V であるため，中間の 1.65V を閾値として設定した．AES 暗号の 10 ラウンド目の入力の 1 バイト目の HW とアラーム信号の ON，OFF との相関係数を求めた．第 4.3 節の相関解析の実験結果と FSA 実験結果を図 4.6 に示す．横軸は各攻撃に用

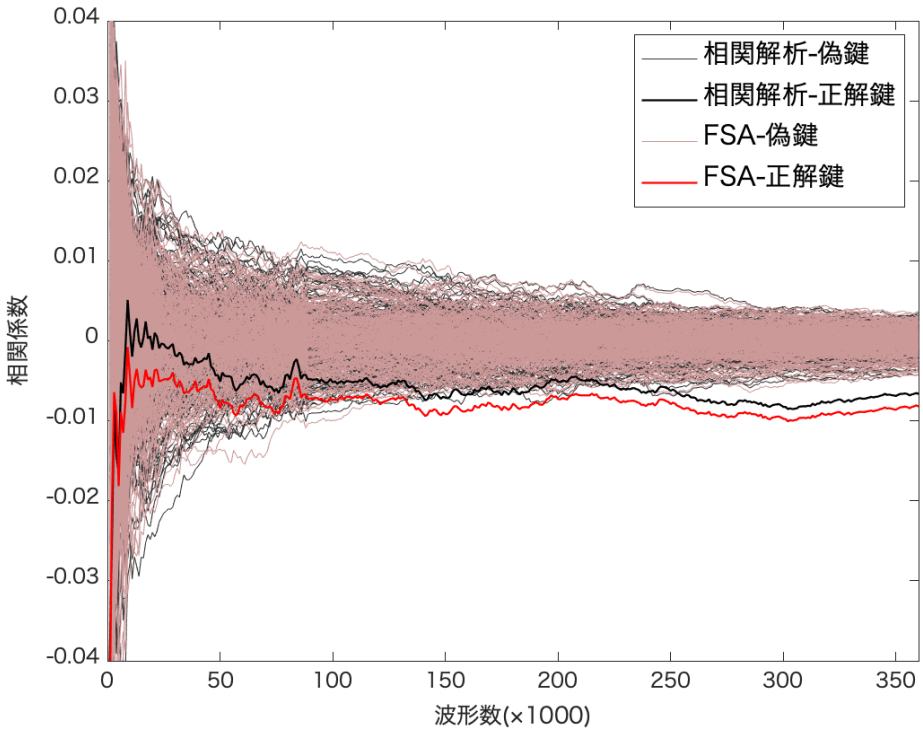

図 4.6：アラーム信号を用いた相関解析と FSA の実験結果

いた波形数を示している．用いた波形数が約 30 万波形以上になると，相関解析と FSA 共に，正解鍵の相関係数が際立って低く，正解鍵が求められることがわかる．この実験より，アラーム信号の ON か OFF という離散的データでも鍵復元できることが示せた．よって，アラーム信号の連続的波形でなくても鍵復元が可能なため，第 4.3 節の相関解析と比較して攻撃者に求める能力が低くなったといえる．

第5章

議論

5.1 アラーム信号と中間値のHWとの依存性に関する考察

第 4.3，4.4 節では，BBICS を統合した AES 暗号チップに対して，相関解析や FSA を行い，鍵復元をした実験について言及をした．チップが相関解析や FSA に対してこのような脆弱性を持つのは，アラーム信号と中間値に相関があるためである．本節では，アラーム信号がなぜ HW に依存するのか考察を行う．

まず，LFI 攻撃されたときの CMOS と BBICS の動作について説明する．BBICS は PMOS につながる pBBICS と NMOS につながる nBBICS の二つのセンサーによって構成されている．本来の BBICS の場合，LFI 攻撃に伴う短絡によって発生する大電流を検知する．CMOS が ON のときであれば，PMOS が ON であり，NMOS が OFF である．このときに NMOS にレーザーが照射される場合を図 5.1 に示す．レーザーが照射され，NMOS が一時的に ON になると，PMOS と NMOS の両方が ON になり，短絡が発生し，nBBICS に大電流が流れる．nBBICS に大電流が流れた後は，第 3.1 節で説明した通りである．このときに LFI 攻撃を検知するのは，nBBICS である．一方，CMOS が OFF のときに攻撃を受け，短絡が発生した場合は pBBICS が LFI 攻撃を検知する．つまり，内部信号の値により，LFI 攻撃を検知するセンサーが異なる．

先行研究では，NMOS と PMOS に対して LFI 攻撃を行った時に，ビットフリップするの

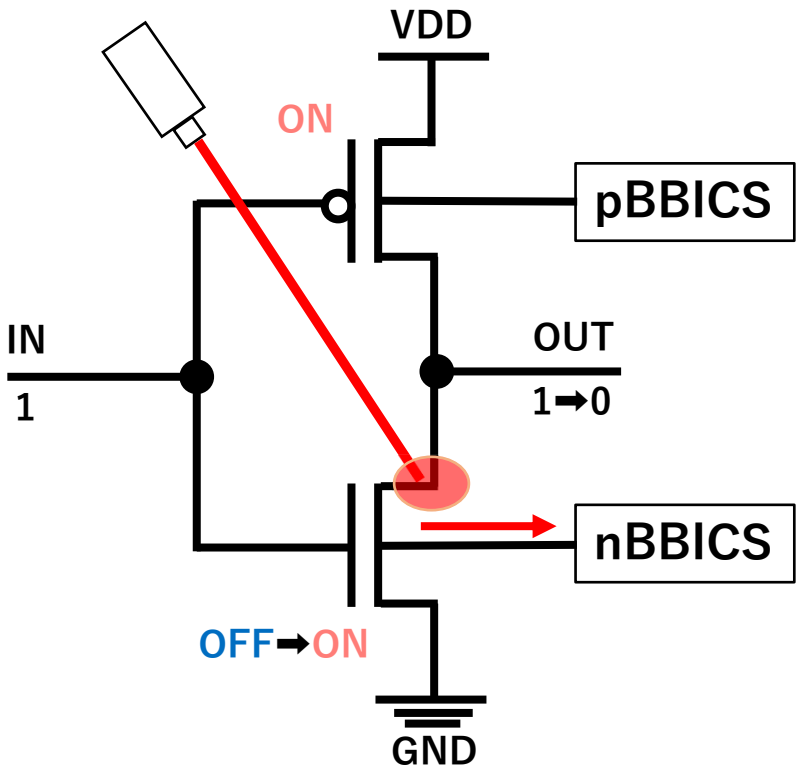

図 5.1：インバータの NMOS に LFI 攻撃をする場合の攻撃検知過程

に必要なレーザーの電力について調査されている [14]．実験結果では，PMOS に LFI 攻撃を行う場合では，NMOS を攻撃対象にしたときと比較して，約 1.2 倍のレーザー電力が必要であると示されている．よって，NMOS と PMOS では LFI 攻撃を受けた時の感度が異なるといえる．また，同じチップ内に存在する NMOS や PMOS でもそれぞれ個体差があることも考えられる．

内部信号の値によって，LFI 攻撃を検知するセンサーが異なることと，NMOS と PMOS の感度が違うことを踏まえて，シミュレーションを実施した．シミュレーションのアルゴリズムを Algorithm2 に示す．X 軸は NMOS と PMOS に流れる電流値の平均の差，Y 軸は NMOS と PMOS にそれぞれに流れる電流値の標準偏差，Z 軸は HW とアラーム信号が出力された回数の相関係数の絶対値を示す．シミュレーションでは，チップ全体にレーザー照射がされたことを想定し，NMOS と PMOS に流れる再結合電流をモデル化している．シミュレーション方法としては，まず X 座標と Y 軸のパラメータに従い，NMOS と PMOS それぞれに流れ

Algorithm 2 アラーム信号と HW との相関関係シミュレーション

Input: NMOS と PMOS に流れる電流値の平均の差 X,NMOS と PMOS に流れる電流値の標準偏差 Y
Output: HW とアラーム信号との相関係数の絶対値 Z

```
1: T ← 80, n_ave ← 50, p_ave ← 50 + X, R ← 正規分布乱数
2: for i = 0 to N do
3:    for HW = 0 to 15 do
4:       for j = 0 to 14 do
5:          if HW > j then
6:             C[j] ← n_ave + Y * R //NMOS に流れる電流値
7:          else
8:             C[j] ← p_ave + Y * R //PMOS に流れる電流値
9:             if max(C[0], C[1], ...C[14]) > T then
10:               countList[HW]++
11:            end if
12:         end if
13:      end for
14:   end for
15: end for
16: return Z ← |ρ(HW,countList)|
```

る電流値を正規分布乱数で決める．次に，HW の値で指定された数の NMOS，PMOS の電流値を選択する．選択された電流値が閾値 T を超えたときに，アラーム信号が出力されるとする．最後に，アラーム信号が出力された回数を求め，HW との相関係数を導出した．

シミュレーション結果を図 5.2 に示す．図 5.2 では，X 軸が正方向にいくにつれて，NMOS と PMOS の感度差があることを示し，Y 軸が正方向にいくにつれて，NMOS 間，PMOS 間の感度の個体差が大きくなることを示す．NMOS に流れる電流値の平均は 50 に設定し，PMOS に流れる電流値の平均は $50+X$ に設定してある．よって，NMOS と PMOS 間の感度差が 1.2 倍になるのは $X = 10$ の位置である．$X = 10$ の位置では，標準偏差が高くなるにつれて，相関係数が高くなっていることがわかる．このことから，PMOS と NMOS に感度差や，PMOS や NMOS に感度の個体差があれば，アラーム信号が出力される頻度は HW と相関することがわかる．よって，相関解析の脆弱性の原因の一つとして，LFI 攻撃を受けた時の PMOS と NMOS に感度差が生じていることが挙げられる．

このシミュレーションでは，以下の 2 つの仮定の上で成り立っている．

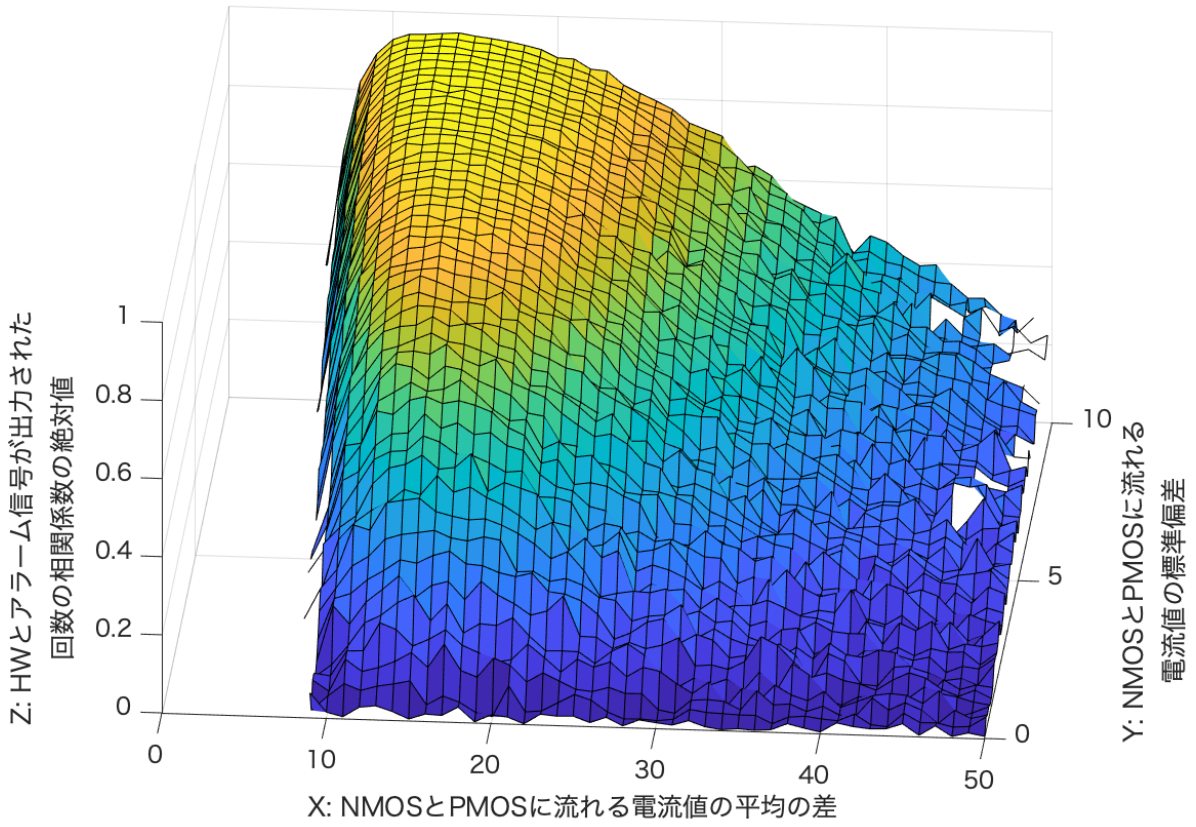

図 5.2 : アラーム信号と HW との相関係数のシミュレーション結果

- PMOS と NMOS に流れる再結合電流は正規分布に基づく
- 内部信号の値によって，LFI 攻撃を検知するセンサーが異なる

仮定のうち，二つ目の仮定は HW に依存する理由を説明する上で不可欠である．本来の BBICS では短絡に伴う大電流を検知する．この場合，内部信号の値によって大電流が流れる MOS が決まる．しかし，実際の BBICS は False negative を防ぐために，十分なマージンをもって検知するように設計されている．具体的には，レーザー照射に伴って PN 接合間に流れる再結合電流でも検知して，アラーム信号を出力する．レーザー照射に伴う再結合電流は NMOS と PMOS のどちらにも流れると考えられる．短絡を検知する場合は，内部信号の値によって LFI 攻撃を検知するセンサーが異なる．しかし，再結合電流を検知した場合，nBBICS と pBBICS のどちらがアラーム信号を出力するかが内部信号の値によって一意に決まるのかは不明である．そのため，再結合電流を検知した場合，内部信号の値によって検知するセンサー

が異なるのか検証する必要がある．検証を行い，シミュレーションにおける 2 つの仮定が満たされれば，PMOS と NMOS との感度差が相関解析の脆弱性の原因として考えられる．

5.2 対策

本章では，第 4.3，4.4 節で提案したアラーム信号を用いた相関解析及び FSA に対する対策を議論する．有効な対策と考えられる手法を二つ提案する．

一つ目の対策は，マスキングなどのサイドチャネル攻撃対策を施すことである．マスキングでは，暗号化計算時の内部信号をランダムな値に変更するため，アラーム信号から中間値情報が漏洩することを防ぐことができると考えられる．よって，サイドチャネル攻撃対策は有効であるといえる．

二つ目の対策は，BBICS 内の nBBICS と pBBICS の感度を一定にするように調整することである．第 5 章の考察より，アラーム信号が中間値の HW に依存するのは，LFI 攻撃を受けた時の NMOS と PMOS の感度が異なることが根本的な原因であると考えられる．よって，対策としては nBBICS と pBBICS の感度を一定にすることが考えられる．感度を一定にするためには，実際に設計されたチップに対し，LFI 攻撃を行い，内部信号の値にかかわらず nBBICS，pBBICS の感度が一定になるようにそれぞれのアラーム信号が出力される電流の閾値を調整する必要がある．

本章で提案した対策についてまとめる．

- マスキングなどのサイドチャネル攻撃対策を施す
- BBICS 内の nBBICS と pBBICS の感度を一定にするように調整する

第6章

LFI攻撃検知技術の特徴

本章では，LFI 攻撃検知技術について整理を行う．LFI 攻撃を検知する技術について，表 6.1 にまとめる．

表 6.1：LFI 攻撃検知技術の特徴

	故障を検知するセンサー・回路	故障要因を検知するセンサー	
		センサーの感度が高い	センサーの感度が低い
例	冗長性をもつ回路，SPB[14]	BBICS[18]	
攻撃耐性	DFA	DFA，IFA	DFA
脆弱性	IFA，FSA	アラーム信号を用いた相関解析，FSA	IFA* アラーム信号を用いた相関解析，FSA
可用性	◎	△ (False positive)	○ (False negative)
コスト	大きい (冗長性をもつ回路の場合，面積や時間+100%)	小さい (面積+28%[18])	

IFA*:センサーの感度によるノイズが多いため，統計的処理を施した IFA

LFI 攻撃検知技術は，その故障自体を検知するものと故障要因を検知するものの二つに大別できる．故障を検知するセンサーや回路は，暗号計算を複数行うような冗長性をもつ回路と SPB[14] があてはまる．故障要因を検知するセンサーには，BBICS があてはまる．BBICS は，設計上，LFI 攻撃に伴う短絡によって発生する大電流を検知するセンサーであり，故障が入らなければアラーム信号を出力しない．しかし，実際に実装された BBICS では，大電流が発生するよりも前の段階でアラーム信号を出力する．第 4.3 節の実験でも言及したように，実験で設定したレーザー照射の強度では，故障が入らなくてもアラーム信号を出力する．よって，設計上の BBICS と実際に実装された BBICS とでは，LFI 攻撃を検知する際の感度が異なるといえる．感度が異なることで，それぞれの攻撃耐性と脆弱性が異なるため，BBICS の中でも区別する必要があると考える．それぞれの特徴を踏まえ，本稿では，設計上の，大電流を検知する BBICS を感度が低いセンサーに区別し，実際に設計された，故障が入らなくてもアラーム信号を出力する BBICS を感度が高いセンサーに区別する．

LFI 攻撃検知技術のそれぞれの耐性と脆弱性について考察を行う．LFI 攻撃検知技術は，故障を検知し，検知した場合に暗号文の出力などを防ぐような設計がされている．そのため，DFA を防ぐことができる．しかし，IFA は故障が発生したか否かという情報を用いて，鍵復元攻撃を行う．IFA の場合，故障の発生有無は，中間値情報に依存する．よって，故障自体を検知するセンサーでは，中間値情報を漏らす可能性があり，IFA は脆弱性として考えられる．先行研究では，SPB に対する IFA が提案されている [30]．IFA と同様に，FSA は故障が発生する感度の情報を用いて攻撃を行うため，故障を検知するセンサー・回路の脆弱性となる．一方，故障要因を検知するセンサーのうち，感度が高いセンサーでは，レーザー照射自体を検知することができるため，検知有無によって中間値情報が漏洩しない．よって，IFA に対して耐性をもつ．しかし，故障要因を検知するセンサーの BBICS では，故障要因を検知した後にアラーム信号を出力する．第 4.3，4.4 節の実験から，このアラーム信号は中間値の情報を漏洩しているといえる．よって，故障要因を検知するセンサーでは，アラーム信号

を用いた相関解析，FSA が脆弱性と考えられる．また，本来の目的である大電流を検知する BBICS を考えた場合，アラーム信号が出力される電流の閾値を，大電流を対象とする設定が想定される．そのときには，[27] で示されたように IFA が可能になるといえる．しかし，実際の設計では，暗号ハードウェアの安全的運用のためにも False negative を回避する必要がある．よって，そのような閾値の設定がされることは考えにくい．また，そのような設計がされたとしても，センサーの感度によって攻撃者が意図しない出力が得られてしまい，ノイズが多く含まれる．そのため，ノイズにも対処できるように，統計的処理を施した IFA が必要となる．それに対し，アラーム信号を用いた相関解析はセンサーの感度に関わらず攻撃することができるため，脅威である．

可用性について考察を行う．故障を検知するセンサー・回路では，故障が生じた場合のみ暗号文の出力を止めることを考えるため，最適な可用性をもつといえる．それに対し，故障要因を検知するセンサーでは可用性が落ちる．特に，センサーの感度が高ければ高いほど，False positive の可能性が高くなり，攻撃者検知には高い能力を有するが，可用性が特に低くなる．

それぞれのコストについては，故障を検知するセンサー・回路が最も大きいといえる．冗長性をもつ回路の場合，面積オーバーヘッドや計算時間が 2 倍になる．それに対し，故障要因を検知するセンサーでは，暗号文を消去する回路を含めても 28%しか面積が増加しない．よって，コストの面では，BBICS は優位なものであると評価できる．

LFI 攻撃検知技術の特徴についてまとめる．LFI 攻撃検知技術では，可用性とコストがトレードオフの関係にあるといえる．また，アラーム信号を用いた相関解析や FSA は，他の攻撃に対し堅牢であると考えられる BBICS に対し，有効な攻撃であると言え，非常に強力な攻撃であると評価できる．それぞれのセンサー・回路において，耐性と脆弱性はそれぞれ異なるため，設計者は，可用性やコストなどを把握した上で，その使用用途にあった LFI 攻撃検知技術を選択することが求められる．

第7章

結論

本論文では，[18] で提案された BBICS を統合した AES 暗号チップのサイドチャネル攻撃耐性の評価を行なった．実験から，アラーム信号を用いた相関解析と FSA によって AES 暗号の秘密鍵を復元できることを示した．脆弱性の原因は，LFI 攻撃を受けた時の NMOS と PMOS の感度が異なることが考えられる．さらにシミュレーションにより，NMOS と PMOS の感度が異なる場合に，アラーム信号と内部信号がどのように相関をするのかを示した．また，アラーム信号を用いた相関解析と FSA を防ぐための根本的な対策を提案した．最後に，LFI 攻撃検知技術の特徴についてまとめ，それぞれのセンサーや回路が持つ耐性や脆弱性を示した．

参 考 文 献

[1] 羽田野凌太, 平田 遼, 松田航平, 三浦典之, 李陽, 崎山一男, “LFI 検知回路に対するサイドチャネル攻撃耐性評価,” 電子情報通信学会論文誌 (A),(accepted).

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” Advances in Cryptology - CRYPTO,vol.1666, pp.388-397, LNCS, 1999.

[3] E. Biham and A. Shamir, “Differential Fault Analysis of Secret KeyCryptosystems,” CRYPTO, Lecture Notes in Computer Science, vol.1294, pp.513-525, Aug.1997.

[4] A. Moradi, M. T. M. Shalmani, and M. Salmasizadeh, “A generalized method of differential fault attack against AES cryptosystem, ” in Proc. CHES'06, pp. 91–100, 2006.

[5] K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, "Information-Theoretic Approach to Optimal Differential Fault Analysis," IEEE Trans. Information Forensics and Security, vol. 7, no. 1, pp. 109-120, Feb. 2012.

[6] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, “Fault Sensitivity Analysis,” In S. Mangard and F.X. Standaert, editors, CHES, volume 6225 of Lecture Notes in Computer Science, pages 320-334. Springer, 2010.

[7] T. Fukunaga and J. Takahashi, “Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers,” Proceedings of the 6th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 84-92, Sept. 2009.

[8] M. Matsubayashi, A. Satoh and J. Ishii, "Clock glitch generator on SAKURA-G for fault injection attack against a cryptographic circuit," 2016 IEEE 5th Global Conference on Consumer Electronics, Kyoto, 2016, pp. 1-4, Oct. 2016.

[9] S. P. Skorobogatov and R. J. Anderson,"Optical Fault Induction Attacks,"CHES, Lecture Notes in Computer Science, vol. 2523, pp. 2-12, Aug. 2002.

[10] Y. Ishai, A. Sahai, and D. Wagner, " Private Circuits: Securing Hardware against Probing Attacks, " CRYPTO, vol.2729, pages 463-481. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[11] H. Tupsamudre, S. Bisht, and D. Mukhopadhyay, " Destroying fault invariant with randomization - A countermeasure for AES against differential fault attacks, " CHES, pp. 93-111, 2014.

[12] Y. Li, K. Ohta, and K. Sakiyama, " Toward Effective Countermeasures Against an Improved Fault Sensitivity Analysis, " IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No.1, pp.234-241, (Jan., 2012).

[13] Y. Li, S. Endo, N. Debande, N. Homma, T. Aoki, T. Le, J. Danger, K. Ohta, and K. Sakiyama,"Exploring the Relations Between Fault Sensitivity and Power Consumption," In Proc. Constructive Side-Channel Analysis and Secure Design (COSADE ' 13), LNCS 7864, Springer-Verlag, pp.137-153 (Mar., 2013).

[14] K. Matsuda, N. Miura, M. Nagata, Y. Hayashi, T. Fujii, and K. Sakiyama, " On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure, " IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), pp. 1-6, Dec. 2016.

[15] L. De Meyer, V. Arribas, S. Nikova, V. Nikov, and V. Rijmen, " MM: Masks and macs

against physical attacks, " CHES, vol. 2019, no. 1, pp. 25-50, 2018.

[16] V. Arribas, T. De Cnudde, and D. Sijacic. Glitch-Resistant Masking Schemes as Countermeasure Against Fault Sensitivity Analysis. In FDTC (2018), IEEE Computer Society, pp. 1-8.

[17] S. Nikova, C. Rechberger and V. Rijmen, " Threshold implementations against sidechannel attacks, "ICICS 2006. LNCS, vol. 4307, pp. 529-545. Springer, Heidelberg (2006).

[18] K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, and N. Miura, " A 286 F^2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser against Laser Fault Injection Attack on Cryptographic Processor, " IEEE J. Solid-State Circuits 53(11): 3174-3182, 2018.

[19] National Institute of Standards and Technology, " FIPS 197:Announcing the Advanced Encryption Standard (AES), " http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, 2001.

[20] Y. Li, R. Hatano, S. Tada, K. Matsuda, N. Miura, T. Sugawara, and K. Sakiyama, " Side-Channel Leakage of Alarm Signal for a Bulk-Current-Based Laser Sensor, " In Proc. International Conference on Information Security and Cryptology (Inscrypt ' 19), LNCS, Springer-Verlag(to appear in Dec., 2019).

[21] G. Piret and J. J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD, " CHES, Lecture Notes in Computer Science, vol. 2779, pp. 77-88, Aug. 2003.

[22] C. Roscian, A. Sarafianos, J. M. Dutertre, and A. Tria, " Fault Model Analysis of Laser-

Induced Faults in SRAM Memory Cells, ” In Proc., Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2013), pp. 89-98, 2013.

[23] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model, ” CHES, pp.16-29, 2004.

[24] T. Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant Software”, Proceedings of CHES 2000, LNCS 1965, pp.238-251 (2000).

[25] F. Schellenberg, M. Finkeldey, N. Gerhardt, M. Hofmann, A. Moradi, and C. Paar, “Large laser spots and fault sensitivity analysis, ”in 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 203-208, 2016.

[26] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A.Sarafianos, “ Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induces currents, ” IEEE International On-Line Testing Symposium (IOLTS), pp. 150-155, July 2015.

[27] T. Sugawara, N. Shoji, K. Sakiyama, K. Matsuda, N. Miura, and M. Nagata, “ Side-Channel Leakage from Sensor-Based Countermeasures against Fault Injection Attack, ” Microelectronics Journal, Vol. 90, pp. 63-71, 2019.

[28] C. Clavier and A. Wurcker, “Reverse Engineering of a Secret AES-like Cipher by Ineffective Fault Analysis,”in Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2013), pp. 119-128, 2013.

[29] Xilinx, ”Spartan-3AN FPGA Family Data Sheet,” https://japan.xilinx.com/support/documentation/data_sheets/ds557.pdf

[30] T. Sugawara, N. Shoji, K. Sakiyama, K. Matsuda, N. Miura, and M. Nagata, "Exploiting Bitflip Detector for Non-Invasive Probing and itsApplication to Ineffective Fault Analysis, " in Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2017), pp. 49-56, 2017.

研究成果・学会発表

学術論文 (査読あり)

- 羽田野凌太, 平田 遼, 松田航平, 三浦典之, 李陽, 崎山一男, “ LFI 検知回路に対するサイドチャネル攻撃耐性評価, ” 電子情報通信学会論文誌 (A),(accepted).

国際学会口頭発表 (査読あり)

- Yang Li, Ryota Hatano, Sho Tada, Kohei Matsuda, Noriyuki Miura, Takeshi Sugawara, and Kazuo Sakiyama, “ Side-Channel Leakage of Alarm Signal for a Bulk-Current-Based Laser Sensor, ” In Proc. International Conference on Information Security and Cryptology (Inscrypt ’ 19), LNCS 12001, Springer-Verlag, pp.346-361, (Dec.,2019).

学会口頭発表 (査読なし)

- 羽田野凌太, 庄司奈津, 李 陽, 菅原 健, 崎山一男, “ AES 暗号への故障差分攻撃のモデル化と攻撃回数の評価, ” IEICE2018 年ソサイエティ大会, (Sep., 2018).
- 羽田野凌太, 李陽, 多田捷, 松田航平, 三浦典之, 菅原健, 崎山一男, “ レーザーフォールト注入攻撃への対策が施された AES 暗号チップの脆弱性評価, ” IEICE2019 年ソサイエティ大会, (Sep., 2019).

- 羽田野凌太, 平田遼, 松田航平, 三浦典之, 李陽, 崎山一男, “レーザー検知回路から漏洩するサイドチャネル情報の考察,”2020 年暗号と情報セキュリティシンポジウム (SCIS2020),3E3-2,7 pages,(Jan.,2020).

その他の発表

- Ryota Hatano and Kazuo Sakiyama, “An Abstraction Model for Differential Fault Analysis on AES,” The First International Workshop on Hardware Oriented Cybersecurity (HwSec2018), (Dec., 19, 2018).

国際会議プロシーディングス (査読あり)(共著)

- Hakuei Sugimoto, Ryota Hatano, Natsu Shoji, and Kazuo Sakiyama, “Validating the DFA Attack Resistance of AES (Short Paper),” In Proc. International Symposium on Foundations & Practice of Security (FPS ’19), LNCS 12056, Springer-Verlag, pp.371-378, (Nov., 2019).

学会口頭発表 (査読なし)(共著)

- 杉本博英, 羽田野凌太, 庄司奈津, 崎山一男, “AES 暗号への 9 ラウンド差分故障解析の攻撃耐性の評価,”IEICE2019 年ソサイエティ大会, (Sep., 2019).

- 平田遼, 羽田野凌太, 李陽, 三浦典之, Svetla Nikova, 崎山一男, “M&M により対策された AES ハードウェアの安全性評価について,”IEICE2020 年ソサイエティ大会, (Sep., 2020).

- 平田遼, 羽田野凌太, 李陽, 三浦典之, 崎山一男, “M&M により対策された AES 暗号

ハードウェアに対するサイドチャネル攻撃,”2021 年暗号と情報セキュリティシンポジウム (SCIS2021), 3D4-4, 6 pages, (Jan., 2021).

謝辞

本研究を進めるにあたり，主任指導教員である電気通信大学情報学専攻崎山一男教授には，長い期間にわたり，常に熱心にご指導をいただき，研究活動を通して様々なことを学ばせていただきました．心より，感謝申し上げます．

同専攻李陽准教授，菅原健准教授には，研究活動に対し，ご指導やご指摘をいただきました．感謝申し上げます．

同専攻太田和夫教授，岩本貢准教授，渡邊洋平助教には，研究内容に対し，適切なご指摘をいただきました．感謝申し上げます．

同専攻崎山研究室，菅原研究室，李研究室の方には大変お世話になりました．感謝申し上げます．

大阪大学情報科学研究科三浦典之教授には，研究内容に対し，多くのご助言とご指摘をいただきました．感謝申し上げます．

最後に，学生生活を支えてくださった両親に感謝申し上げます．